REMARKS

Claims 1-35 are all the claims pending in the application.

Claims 1-35 are rejected.

Claims 1-22, 24-25, 28, 30 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Giniger et al. (U.S. Patent No. 6,751,729).

Claims 23, 26-27, 29, 31-32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Giniger et al. (U.S. Patent No. 6,751,729) in view of Rueda et al. (U.S. Publication No. 2002/0112076).

The Applicants traverse the rejections and request reconsideration.

The Applicants amend the claims to further clarify that the terminal does not have direct access to the wide area network.

Giniger suggests a conventional virtual private network setup. The virtual network is established between a plurality of "edge devices" (or "node devices" as noted in the summary of invention). **The edge device acts as an intermediary between a local network of computers and the VPN.** Thus, a packet from a user computer device would travel through the local network, arrive at the edge device, and the edge device would intelligently decide which VPN tunnel to send it through so as to arrive to its destination. The edge devices include cryptographic modules so as to ensure that the tunnels established between the edge devices are secure. In Giniger specific manufacturing rules are provided for ensuring that the cryptographic certificates are stored in a tamper-resistant portion of the edge device.

The present invention is completely different from Giniger.

In the present invention, the edge device is assumed to be completely untrustworthy. It cannot be trusted to hold a cryptographic certificate; it cannot be trusted to establish and maintain a VPN tunnel. For example, a WiFi router at a coffee shop or at someone's home cannot be trusted to hold the certificate. A conventional solution would be to move the functionality of the "edge device" back to the client station. In other words, in such a conventional solution, the user's computer would act as the edge device and would manage the secure tunnel. Most conventional VPNs are believed to operate in this fashion.

However, such a conventional solution has significant problems. Specifically a user would need to "connect" his computer to a local network and get full access privileges to the local network and the Internet. The user computer receives an IP address using which the user accesses the Internet. Once the VPN client is fired up to connect to the VPN, all the traffic goes through the VPN tunnel to a node in the VPN network. In such a case, access to the Internet is also through the gateway in the VPN, not through the local network's connection.

On the other hand, the present invention assumed that you, as a "guest" of the local network, have no real interest in gaining full access to the Internet through the local network and its IP address. What you want is access to your own "home" VPN network using your own IP address.

So, the protocol according to the present invention is as follows:

1. User computer sends a special message to the edge device which says I want the special service. The edge device provides a "fake" IP address back which need only be usable for the present invention.

2. The edge device will then proceed to mediate a connection between a node in the VPN and the user. Since the connection can be eavesdropped by the edge device, additional precautions such as using public key cryptography or any important authentication messages that pass between you and your VPN node are provided.

3. If the user is approved, the node and the computer establish a VPN tunnel between the user and the VPN network through the edge device. If not, the connection is cut off.

In the present invention, the edge device does not need to be trusted.

Specifically, the present inventive combination including the feature that a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet (as in independent claims 1, 4, 5 and 6) is not suggested by Giniger.

Claims 2, 3, 7-22, 24-25, 28, 30, 33 and 35 are dependent on claims 1, 4, 5 or 6 and are allowable at least for the same reasons.

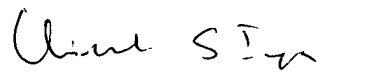
Claims 23, 26-27, 29, 31-32 and 34 are dependent on claims 1, 4, 5 or 6 and are allowable at least for the same reasons. Further, Rueda does not overcome the deficiencies noted in the teachings of Giniger.

New claims 36-41 are provided for examination. Claim 36 includes the feature that a connection is established between the authentication server and the terminal for trusted network services without providing the terminal with direct access to the wide area network. As noted above, Giniger does not disclose (or suggest this feature).

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Chid S. Iyer
Registration No. 43,355

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 13, 2006